IT-Sicherheit in Produktionsanlagen

Eine Einführung für kleine und mittlere Unternehmen

Prof. Dr. Karl-Heinz Niemann - Hannover

Prof. Dr. Karl-Heinz Niemann
Email: Karl-Heinz@Niemann-on-line.de

In Kooperation mit WAGO Kontakttechnik GmbH & Co. KG

Inhaltsverzeichnis

1. Einführung

Dieses Dokument befasst sich mit der IT-Sicherheit von Produktionsanlagen. Es richtet sich an kleine und mittlere Unternehmen, welche auf der Suche nach einem einfachen Vorgehensmodell für die Sicherstellung der IT-Sicherheit im Produktionsbereich sind.

Um Leser für die Notwendigkeit der IT-Sicherheit von Produktionsanlagen zu sensibilisieren, werden in Kapitel 2 Sicherheitsvorfälle dargestellt. Es zeigt sich, dass Cyber-Angriffe auf Produktionsanlagen heute kein Zufall mehr, sondern auf einem gezielten Vorgehen beruhen.

Danach folgt in Kapitel 3 ein Überblick über die wichtigsten Normen und Empfehlungen zum Themenfeld „IT-Sicherheit in der Produktion".

Kapitel 4 entwickelt an Hand eines Zehn-Punkte-Plans ein Konzept für den Aufbau eines IT-Sicherheitssystems für kleine und mittlere Unternehmen (KMU). Dabei liegt der Schwerpunkt nicht nur auf den technischen, sondern insbesondere auch auf den häufig vernachlässigten organisatorischen Maßnahmen.

Abschließend gibt Kapitel 5 einen Ausblick auf künftige Anforderungen und Lösungen im Kontext von Industrie 4.0

2. Der aktuelle Stand der IT-Sicherheit in automatisierungstechnischen Anlagen

Dieses Kapitel gibt einen Überblick über den aktuellen Stand der IT-Sicherheit in der Produktion. Ausgehend von bekannten Sicherheitsvorfällen werden die Herausforderungen für aktuelle Produktionsanlagen abgeleitet. Die Top-10-Bedrohungen des BSI dienen hierfür als Basis.

2.1. Bekannte Sicherheitsvorfälle in Produktionsanlagen

Die Anforderungen in Bezug auf die IT-Sicherheit in der Produktion ändern sich stetig. In der Vergangenheit waren IT-Sicherheitsvorfälle in der Produktion in der Regel „Kollateralschäden" gewöhnlicher Schadsoftware, die zufällig in eine Produktionsanlage geraten ist. Einer der ersten bekannten Vorfälle dieser Art war der Befall verschiedener Werke der Firma Daimler Chrysler im Jahr 2005 durch die Schadsoftware „Zotob" [PAK2005]. Dabei waren weltweit 13 Werke des Unternehmens betroffen. Der entstandene Schaden wird auf 14 Mio. US$ geschätzt [BYR2009].

Neuere Vorfälle zeigen, dass zunehmend auch Schadsoftware zum Einsatz kommt, die sich explizit gegen Produktionsanlagen richtet. Der bisher prominenteste Fall „Stuxnet" [FAL2011] [LAN2013] richtete sich gegen eine iranische Anreicherungsanlage für Uran. Die U.S.A und Israel werden in diesem Fall als vermutliche Urheber genannt [BRO2011]. Daneben sind weitere Vorfälle dokumentiert, die keiner staatlichen Intervention zugeordnet werden können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet zum Beispiel von einem dedizierten Angriff auf einen Hochofen in Deutschland, der zu dessen Havarie führte [BSI2014e]. Darüber hinaus existiert inzwischen Schadsoftware, die gezielt Komponenten von Automatisierungssystemen angreift. Das ICS-CERT beschreibt zum Beispiel eine Schadsoftware, welche OPC-Server befällt [CERT2014].

Eine neue Dimension von Cyber-Angriffen auf Automatisierungssysteme und kritische Infrastruktur markiert ein Angriff auf das Energieversorgungssystem der Ukraine am 23.12.2015 [CERT2016]. Nahezu zeitgleich wurden drei Energieversorger angegriffen, was zu einem Ausfall der Energieversorgung für 225 000 Kunden führte. Bei dem Angriff wurden Leistungsschalter im Energieversorgungsnetz durch Remote-Zugriff unkontrolliert bedient. Gleichzeitig wurden auf Steuerungsrechnern Datenbestände gelöscht.

Neben industriellen Automatisierungssystemen sind Komponenten der Gebäudeautomation in gleicher Art betroffen. Im Jahr 2013 wurde ein Fall dokumentiert bei dem

Heizungsanlagen ohne ausreichenden Schutz zum Zwecke der Fernwartung mit dem Internet verbunden wurden [EIK2013] [STA2013a]. Durch eine mangelnde Absicherung konnten externe Personen Zugriff auf diese Anlagen erhalten. Trotz Veröffentlichung der Schwachstelle in der Fachpresse und Behebung durch den Hersteller, waren auch nach zwei Jahren noch eine große Zahl von verwundbare Heizungsanlagen im Internet ungeschützt zugänglich [STA2015]. Die Nutzer haben die bereitgestellten Sicherheitsupdates nicht installiert, die Geräte sind weiterhin verwundbar.

Auch der maritime Sektor muss sich den Herausforderungen der Cyber-Security stellen. Die auf Schiffen eingesetzten Automatisierungssysteme sind zwar für diesen speziellen Einsatzzweck ertüchtigt und zertifiziert, dennoch basieren sie in der Regel auf konventionellen Automatisierungssystemen. Somit gelten für diese Systeme die gleichen Bedrohungen, wie auch für konventionelle Automatisierungssysteme [JEN2015]. Durch zusätzliche elektronische Systeme für die Navigation und Kollisionsvermeidung wird die Angriffsfläche für potentielle Angreifer zudem größer [DIR2015].

Im Weiteren wird sich dieses Dokument mit produktionstechnischen Anlagen der Prozess- und der Fertigungsindustrie befassen.

2.2. Künftige Herausforderungen an die IT-Sicherheit in der Produktion

Es ist davon auszugehen, dass sich die künftige die Bedrohungslage für Automatisierungssysteme weiter zuspitzen wird. Darauf weist die Anzahl und Entwicklung im Zeitablauf der dokumentierten Angriffe hin. Die mit Industrie 4.0 einhergehende zunehmende Vernetzung zur Realisierung einer horizontalen und vertikalen Integration von Produktionsprozessen wird zu weiteren Angriffsmöglichkeiten führen. In einer repräsentativen Umfrage des Allensbacher Instituts nennen 88% der befragten Führungskräfte einen wirksamen Schutz gegen Cyber-Angriffe als die größte Herausforderung bei der Einführung von Industrie 4.0 [DEU2015].

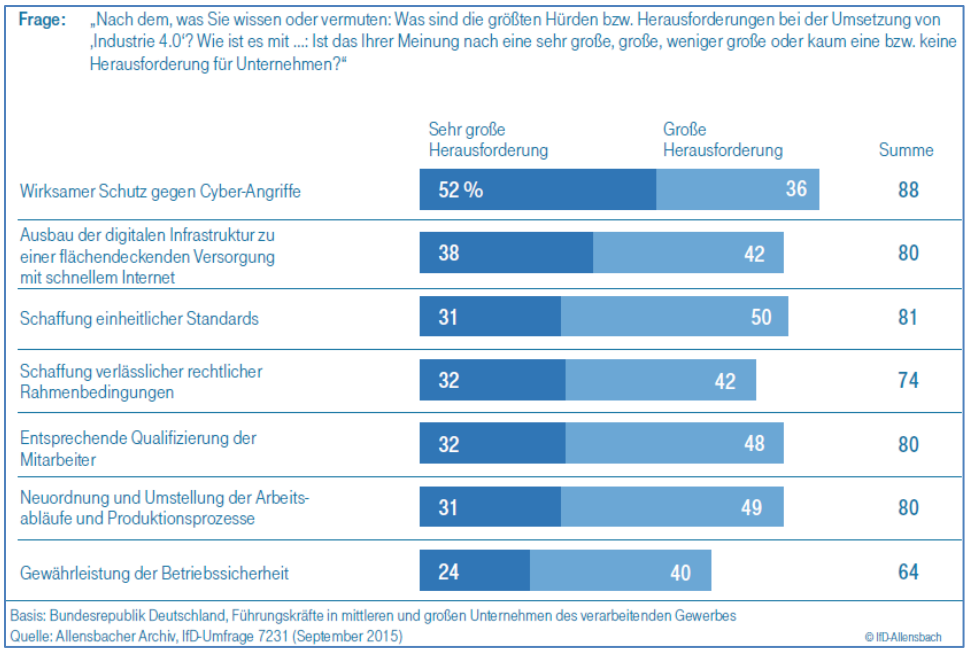

Abbildung 1: Hürden und Herausforderungen bei der Umsetzung von Industrie 4.0 [DEU2015]

Das Bundesamt für Sicherheit in der Informationstechnik gibt in regelmäßigen Abständen eine Liste der Top-10-Bedrohungen für Automatisierungssysteme heraus. Die aktuelle Ausgabe [BSI2016a] nennt die in Tabelle 1 genannten Bedrohungen und deren Platzierung

Platz	Bedrohung	Handlungsfelder
1	Social Engineering und Phishing	Mensch, Prozesse
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Prozesse, Technik
3	Infektion mit Schadsoftware über Internet und Intranet	Netzwerk, Technik
4	Einbruch über Fernwartungszugänge	Prozesse, Netzwerk
5	Menschliches Fehlverhalten und Sabotage	Mensch, Prozesse
6	Internet-verbundene Steuerungskomponenten	Netzwerk, Technik
7	Technisches Fehlverhalten und höhere Gewalt	Technik
8	Kompromittierung von Extranet und Cloud-Komponenten	Netzwerk, Technik
9	(Distributed) Denial of Service Angriffe	Netzwerk, Robustheit
10	Kompromittierung von Smartphones im Produktionsumfeld	Mensch, Prozesse, Technik

Tabelle 1: Top-10-Bedrohungen erweitert um Handlungsfelder

Es ist zu erkennen, dass die genannten Top-10-Bedrohungen verschiedenen Angriffsarten und damit Handlungsfeldern zuzuordnen sind. Angriffe können auf verschiedenem Weg erfolgen: Z. B. über das Netzwerk, über kompromittierte Komponenten (USB-Sticks, Smartphones) aber auch über Social Engineering oder Phishing. Die

Überlastung von Komponenten oder Netzwerken durch eine Flut unsinniger Anfragen (Denial of Service, Distributed Denial of Service) stellt ebenfalls eine Angriffsart dar. Basierend auf den beschriebenen Bedrohungen sollen nun im nächsten Abschnitt die Handlungsfelder für die Implementierung eines IT-Sicherheitskonzeptes für Produktionsanlagen abgeleitet werden.

2.3. Handlungsfelder in Bezug auf die IT-Sicherheit in der Produktion

Zur Verdeutlichung der Handlungsfelder hat der Autor Tabelle 1 um die rechte Spalte mit Handlungsfeldern erweitert. Einzelne Themen sind einem oder mehreren Handlungsfeldern zuzuordnen, die im Folgenden kurz beschrieben werden:

- **Mensch:** Der Mensch betreibt und überwacht die Produktionsanlage und soll für deren Sicherheit sorgen. Gleichzeitig stellt der Mensch einen Schwachpunkt in Bezug auf die IT-Sicherheit dar. Über Social Engineering und Phishing kann er ungewollt Dritten einen Zugang zur Anlage ermöglichen. Im Falle von Fehlverhalten oder Sabotage kompromittiert der Mensch gewollt oder ungewollt die IT-Sicherheit der Anlage.
- **Technik**: Die eingesetzte Technik (Steuerungskomponenten, Netzwerkkomponenten) muss gegen Angriffe geschützt sein. Schwachstellen, die bekannt sind, müssen zeitnah behoben werden. Eine regelmäßige Kommunikation mit dem Hersteller der Komponenten, z. B. durch Abonnieren von Security Alerts ist sinnvoll.
- **Prozesse**: Nicht alle Aspekte der IT-Sicherheit lassen sich über Technik lösen. In vielen Fällen sind neben der Technik entsprechende Prozesse (Regeln, Vorschriften) zu definieren. Die Mitarbeiterinnen und Mitarbeiter sind in diesen Prozessen regelmäßig zu schulen. Die Beachtung der Prozesse ist zu überwachen und ggf. auftretendes Fehlverhalten zu sanktionieren. Dadurch steht dieser Punkt in Beziehung zum Punkt „Mensch“.
- **Netzwerk**: Obwohl das Kommunikationsnetzwerk einer Produktionsanlage der Technik zuzuordnen ist, wird es hier separat genannt. Gerade das Netzwerk stellt in vielen Fällen **das** Einfallstor für Angriffe dar. Hier ist ein besonderes Augenmerk erforderlich, um das Produktionsnetzwerk vom Rest des Firmennetzes und insbesondere vom Internet ausreichend gut abzuschotten.
- **Robustheit:** Denial of Service Angriffe bzw. Distributed Denial of Service Angriffe werden in der Regel über das Internet gegen ein Unternehmen gerichtet und treffen zunächst den äußeren Perimeter des Unternehmens. Auch wenn ein Durchbruch eines solchen Angriffs bis zur Produktionsanlage das Durchdringen weiterer Perimeter erfordert, müssen Automatisierungssysteme dennoch eine gewisse Robustheit gegenüber Überlastsituationen aufweisen.

Die beschriebenen Handlungsfelder zeigen, dass die IT-Sicherheit für Produktionsanlagen kein ausschließlich technisches Problem ist. Schwachstellen können neben technischen Problemen (Schwachstelle in Software, nicht eingespielter Software-Patch) auch organisatorische Unzulänglichkeiten (Mitarbeiter wissen nicht, dass bestimmte Dinge unzulässig sind, Regelung des Zugangs zu Anlagenkomponenten) sein.

Aus dieser Sachlage kann folgender Handlungsbedarf abgeleitet werden. Das IT-Sicherheitskonzept einer Produktionsanlage muss neben den technischen Aspekten und Aspekten der Netzwerkkommunikation auch organisatorische und soziale Aspekte (Verhalten des Menschen, Fehlverhalten des Menschen) berücksichtigen. Erst ein strukturierter und geschichteter Ansatz, der alle Aspekte ganzzeitlich berücksichtigt kann eine optimale Absicherung der Anlage gewährleisten. Ein solcher Ansatz wird mit dem Begriff „Defense in Depth“ [DHS2016b] beschrieben.

Gerade für kleine und mittelständische Unternehmen (KMU) ist die Planung, Implementierung und der dauerhafte Betrieb eines Defense in Depth Konzeptes keine einfache Aufgabe. Das erforderliche Knowhow zum Aufbau ist hoch. Die Ressourcen im Unternehmen hierfür sind in der Regel knapp oder verfügen nicht über die erforderliche Ausbildung auf diesem speziellen Gebiet. Daher sind künftige Konzepte erforderlich, welche auch für KMU wirtschaftliche und trotzdem sichere Lösungen liefern.

3. Normen, Standards, Richtlinien und Gesetze

Im Bereich der IT-Sicherheit stehen Unternehmen eine Reihe von Normen bzw. Normreihen zur Verfügung. Die Normen definieren den Stand der Technik und ermöglichen so eine standardisierte Vorgehensweise in Bezug auf Auslegung, Implementierung, Betrieb und Zertifizierung von IT-Sicherheitssystemen.

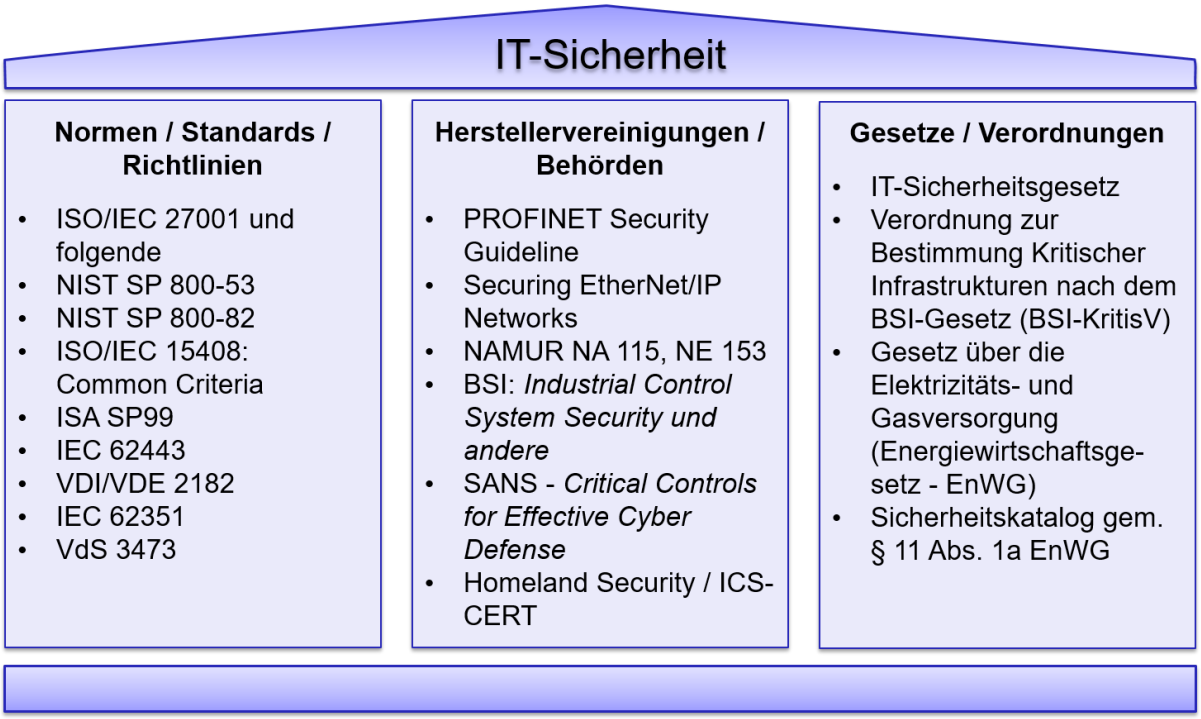

Abbildung 2: Übersicht über Normen und Standards zur IT-Sicherheit

Abbildung 2 gibt einen Überblick über Normen und Standards zur IT-Sicherheit. Neben Normen und Standards für den Office-Bereich (ISO 27000-Reihe, IEC 15408, BSI-Grundschutzkatalog) sind auch Normen aufgeführt, die speziell den Produktionsbereich (ISA SP99/IEC62443, IEC 62351, VDI/VDE 2189) adressieren. Die Aufstellung wird ergänzt um eine Reihe von Standards von Hersteller-/Anwendervereinigungen (PROFINET, EtherNet/IP, NAMUR) und Behörden (BSI, Homeland Security)

Die folgenden Abschnitte liefern einen Überblick über den Stand der Normung. Dabei werden zunächst die allgemeinen Normen für die IT-Sicherheit betrachtet. Im Anschluss folgt ein Überblick über spezielle Normen für die Automatisierungstechnik und Empfehlungen von Herstellerorganisationen. Das Kapitel endet mit einem Ausblick auf das IT-Sicherheitsgesetz.

3.1. Normen und Standards für den Office Bereich

Die IT-Sicherheit im Office-Bereich ist schon seit vielen Jahren über entsprechende Normen definiert. Die Normreihe ISO 27000 liefert hier einen umfassenden Satz an Normen, welche neben technischen Aspekten auch die zugehörigen Prozesse beschreiben. Eine Übersicht über die Normreihe findet sich z. B. in [KER2016]. IT-Sicherheitssysteme lassen sich auch gemäß der Norm entsprechend zertifizieren. Die Vorgehensweise bei der Zertifizierung findet sich z. B. in [KER2013]. Eine Zertifizierung nach der Normreihe ISO 27000 wird als komplex und aufwendig empfunden. Daher sind hauptsächlich Unternehmen zertifiziert, die als besonders exponiert gelten (Banken, Zahlungsdienstleister). KMUs verfügen üblicherweise über kein zertifiziertes IT-Sicherheitssystem nach ISO 27000.

Basierend auf der ISO 27000-Normreihe hat das Bundesamt für Sicherheit in der Informationstechnik eine Reihe von Grundschutzkatalogen [BSI2016c] definiert, welche einen vereinfachten Zugang zur Norm ermöglichen. Darüber hinaus stellt das BSI passende Checklisten und Erhebungsbögen bereit. Das erlaubt KMUs einen einfacheren Zugang zum Thema der IT-Sicherheit.

Der VDS bietet mit der Richtlinie [VDS_3473] ein Leitlinie für die Cyber-Security im Office-Bereich, welche auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten ist. Eine Zertifizierung nach diesem Standard ist möglich. Der Aufwand ist auf die Bedürfnisse von KMU zugeschnitten und liegt deutlich unter dem einer Zertifizierung nach der ISO 27000-Normreihe.

3.2. Normen und Standards für den Produktionsbereich

Die in Kapitel 3.1 beschriebenen Normen adressieren die IT-Sicherheit im Office-Bereich. Damit ist die IT eines Unternehmens gemeint welches über keine Produktionsanlagen verfügt (z. B. Banken) oder der Teil eines Unternehmens, in dem keine Produktionsanalagen angesiedelt sind (z. B. Verwaltung, Vertrieb Personalabteilung, etc.). Die Anforderungen im Office Bereich sind wie folgt priorisiert: Vertraulichkeit, Integrität und Verfügbarkeit. Abbildung 3 zeigt auf der linken Seite die Priorisierung dieser Schutzziele für den Office-Bereich.

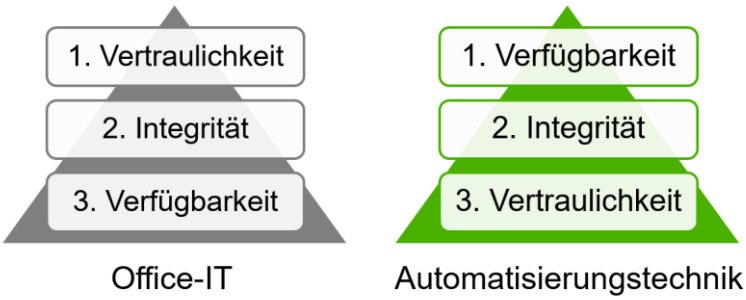

Abbildung 3: Priorisierung der Schutzziele für Office IT und Automatisierungstechnik

Im Produktionsbereich ist die Priorisierung eine andere. Wie in Abbildung 3 auf der rechten Seite zu sehen ist, hat hier die Verfügbarkeit der Produktionsanlage die höchste Priorität, gefolgt von der Integrität der Anlage. Die Vertraulichkeit folgt erst an dritter Stelle.

Auf Grund dieser Priorisierung und auf Grund des für Produktionsanlagen in vielen Bereichen erforderlichen Echtzeitverhaltens sind die in Kapitel 3.1 beschriebenen Normen nicht oder nur eingeschränkt auf den Produktionsbereich anwendbar. Aus diesem Grund ist eine Reihe von Normen in der Entwicklung, welche die Anforderungen der Produktion berücksichtigen. Die folgenden Abschnitte stellen die wichtigsten dieser Normen vor.

3.2.1. IEC 62443 Normreihe

Die Normreihe IEC 62443 wird von der Internationalen elektrotechnischen Kommission (IEC) und der International Society of Automation (ISA) entwickelt. Die ersten Arbeiten an der Norm wurden in der Arbeitsgruppe ISA SP99 gestartet und werden zurzeit in einer Kooperation aus IEC und ISA fortgeführt. Daher finden sich in vielen Dokumenten noch Referenzen auf Arbeitsgruppen und Dokumente der ISA.

Basierend auf den Modellen und Anforderungen der ISO 27000 Normreihe werden in der IEC 62443 Normreihe die speziellen Anforderungen der IT-Sicherheit im Produktionsbereich berücksichtigt. Abbildung 4 zeigt die Struktur der Normreihe.

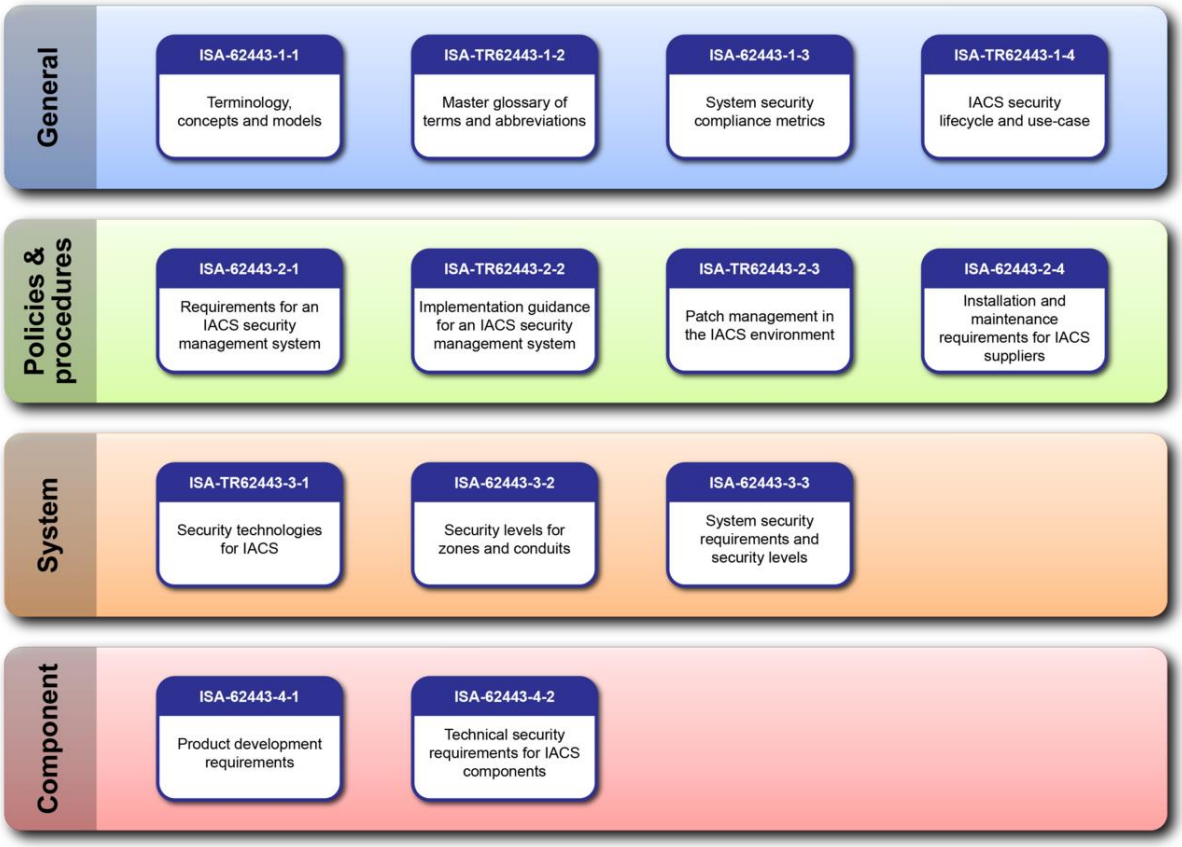

Abbildung 4: Teile der IEC 62443 [Bildquelle: Wikimedia Commons]

Die Norm-Reihe IEC 62443 besteht aus vier Hauptbereichen, die im Folgenden einschließlich der zugeordneten Normen vorgestellt werden:

- Im Teil **„General"** werden in [IEC_62443_1_1] zunächst Begriffe, Konzepte und Modelle definiert. Der Teil [IEC_62443_1_2] stellt definiert alle Begriffe, die in den Normen verwendet werden. Der Teil [IEC_62443_1_3]definiert Metriken für die Bewertung der IT-Sicherheit, im Teil [IEC_62443_1_4] werden der Sicherheitslebenszyklus und Anwendungsfälle beschrieben.

- Der Teil **„Policies & Procedures**" beschreibt das IT-Sicherheits-Management-System und definiert damit die Organisation der IT-Sicherheit, gefolgt von Implementierungshilfen. Der Teil [IEC_62443_2_1] beschreibt Anforderungen an ein IT-Sicherheits-Managementsystem, z. B die Definition von Security Prozeduren. Der Teil [IEC_62443_2_2] gibt Hinweise, wie und in welchen Bereichen diese Prozeduren zu implementieren sind. Das Aktualisieren der Software von Automatisierungssystemen, das Patchen, ist von besonderer Bedeutung, weil es bei unsachgemäßem Vorgehen zu Betriebsstörungen kommen kann. Daher widmet der Standard dem Patch-Management einen eigenen Teil [IEC_62443_2_3]. Der Teil [IEC_62443_2_4] befasst sich mit dem Einsatz von Dienstleistern für Inbetriebnahme und Service aus Sicht der IT-Sicherheit.

- Im Teil **„System“** wird das technische Vorgehen beschrieben. Der Teil [IEC_62443_3_1] beschreibt zunächst die zu Grunde liegenden Technologien wie z. B. Authentifizierung, Verschlüsselung, Filterung und Logging. Der Teil [IEC_62443_3_2] beschreibt die Strukturierung einer Anlage in Zonen (abgeschottete Bereiche) und Conduits (gesicherte Verbindungen zwischen den Bereichen). Damit soll eine automatisierungstechnische Anlage in Teilbereiche unterteilt werden, die wiederum gegeneinander abgeschottet sind. Der Teil [IEC_62443_3_3] definiert eine Metrik zur Bewertung des erreichten Sicherungszustandes durch die Einordnung der realisierten Lösung in Security Level.

- Im Teil **„Component“** werden die Anforderungen an die Komponenten und den zugehörigen Entwicklungszyklus beschrieben. Dieser Teil richtet sich an die Hersteller von Automatisierungssystemen. Der Teil [IEC_62443_4_1] definiert den Entwicklungsprozess, der bei der Entwicklung von Komponenten für die Automatisierungstechnik zu beachten ist. Hierbei sind z. B. Themen wie: "Security Management Process", "Security Requirement Specification", "Secure Architecture Design" sowie "Security Risk Assessment and Threat Modelling" Bestandteil der Norm. Der Teil [IEC_62443_4_2] beschreibt die technischen Anforderungen für die Komponenten von Automatisierungssystemen, Applikation und Funktionen.

Die Normen sind bisher nur zum Teil veröffentlicht. Alle Teile der Normreihe liegen jedoch zumindest als Entwurf vor. Der aktuelle Stand der Arbeiten und der Freigabestatus der Normteile kann unter [ISA2016] eingesehen werden. In [KOB2016] wird ein Überblick über die Normreihe IEC 62443 gegeben und die Zusammenhänge zwischen den Normteilen werden erläutert. Die beschriebenen Normen, bzw. Normentwürfe umfassen zur Zeit 1018 Druckseiten (Stand Nov. 2016).

3.2.2. VDI/VDE 2182 Normreihe

Mit der Normreihe VDI/VDE 2182 wird das Thema IT-Sicherheit für Produktionsanlagen an praktischen Beispielen für die Fertigungs- und die Prozessindustrie verdeutlicht. Dabei werden die Sichten für Hersteller, Integratoren und Betreiber adressiert.

Der Teil 1 der Norm [VDI_2182_1] definiert zunächst die wesentlichen Begriffe der IT-Sicherheit für Produktionsanlagen:

- Benutzer
    - Person oder Anwendung, die mit dem Betrachtungsgegenstand interagieren können.

- Asset
  - Alle materiellen und immateriellen Werte von Automatisierungsgeräten, Automatisierungssystemen, Maschinen oder Produktionsanlagen, die bedroht sein können und die schützenswert sind
  - Beispiele: SPS, Rezeptur, Schnittstellenfunktionen, Firmware.
- Bedrohung
  - Ein Umstand oder ein Ereignis, durch den oder das ein Schaden entstehen kann.
- Risiko
  - Kombination von Wahrscheinlichkeit und Ausmaß eines Schadens.
- Risikoreduzierung
  - Senkung der Schadenswahrscheinlichkeit oder der Schadenshöhe durch Anwendung von Schutzmaßnahmen.
- Schwachstelle
  - Mangel, der dazu führt, dass eine Bedrohung für den Betrachtungsgegenstand wirksam werden kann.
- Verursacher
  - Autorisierter oder nicht-autorisierter Benutzer, dessen Aktionen beabsichtigte oder unbeabsichtigte negative Auswirkungen auf Schutzziele eines Betrachtungsgegenstands haben können.

Danach definiert die Norm ein Vorgehensmodell mit zugehörigen Rollen, wie es in Abbildung 5 dargestellt ist.

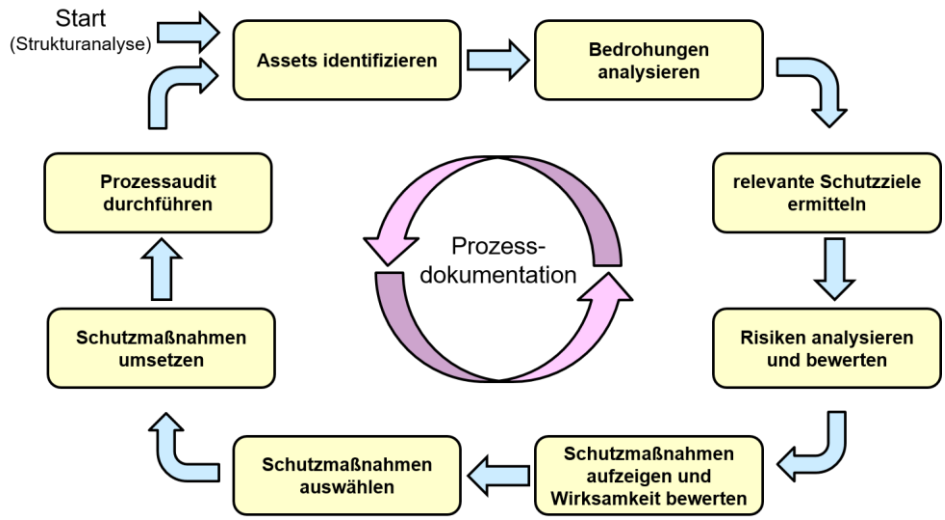

Abbildung 5: Vorgehensmodell nach [VDI_2182_1]

Das Vorgehensmodell der VDI/VDE 2182 orientiert sich an einem so genannten „Plan-Do-Check-Act-Zyklus“ (PDCA).

1. In einem ersten Schritt werden die Assets der Anlage, insbesondere Automatisierungskomponenten, Rechner, Server, etc.) identifiziert und aufgenommen. Das Ergebnis ist eine Liste der identifizierten Assets.
2. Als nächstes sieht der Zyklus vor, die Bedrohungen, welche auf die Assets wirken, zu identifizieren. Dabei werden Bedrohungsszenarien betrachtet und dokumentiert. Die VDI/VDE 2182 gibt dabei entsprechende Templates vor.
3. Im dritten Schritt sieht die Norm die Ermittlung der relevanten Schutzziele vor. Abgeleitet aus den Bedrohungen, werden für jedes Asset die Schutzziele festgelegt und dokumentiert.
4. Der vierte Schritt des Vorgehensmodells sieht nun eine Risikobewertung vor. Basierend auf den Bedrohungen und den identifizierten Schutzzielen werden nun die Wahrscheinlichkeit des Eintretens der identifizierten Bedrohungen und ein zugeordneter potentieller Schaden beschrieben. Aus der Kombination von Eintrittswahrscheinlichkeit und Schadenshöhe kann ein zugeordnetes Risiko identifiziert werden.
5. Das Ergebnis der Risikobewertung identifiziert Felder in denen das bestehende Risiko nicht akzeptabel ist. Hier sind Maßnahmen zur Risikoreduzierung, so genannten Schutzmaßnahmen, vorzusehen und in Bezug auf ihre Wirksamkeit und Wirtschaftlichkeit zu bewerten.
6. Basierend auf den Betrachtungen aus Schritt 5 erfolgt nun die Auswahl der Schutzmaßnahmen. Ziel dieser Auswahl ist es, in einem wirtschaftlich vertretbaren Rahmen Schutzmaßnahmen zu implementieren und gleichzeitig die erforderliche Risikoreduzierung zu erreichen.
7. Der nachfolgende Schritt sieht die Umsetzung der ausgewählten Schutzmaßnahmen vor.
8. Auf Basis der vorangehenden Schritte erfolgt abschließend ein Audit des beschriebenen Vorgangs. Hierbei werden die erstellten Dokumente sowie die Wirksamkeit der beschriebenen Schutzmaßnahmen ermittelt. Das Audit sollte von Personen durchgeführt werden, die nicht an den vorangehenden Schritten beteiligt waren.

Da sich die Bedrohungslage für eine Produktionsanlage durch externe Ereignisse ändern kann, sollte dieser Prozess in bestimmten Zeitintervallen wiederholt werden.

Zur Unterstützung des beschriebenen Prozesses stehen SW-Werkzeuge zur Verfügung, welche die Erfassung und Bewertung der Assets unterstützen. So stellt das Bundesamt für Sicherheit in der Informationstechnik das Werkzeug LARS [BSI2014a], zur Verfügung. Die Homeland Security bietet das Werkzeug CSET [ICS2016] an. Das Forschungsprojekt INSA [GLA2015] verfolgt den Ansatz einer automatisierten Bedrohungsanalyse.

Die VDI/VDE 2182 Normreihe definiert den Prozess in Bezug auf drei Rollen:

- Hersteller: Die Hersteller entwickeln und vertreiben die Anlagenkomponenten. Sie sind gleichzeitig für die Wartung und Pflege der gelieferten Komponenten (z. B. SW-Updates zum Beheben von Sicherheitslücken) zuständig.
- Integrator: Der Integrator ist ein vom Betreiber beauftragter Dienstleister der für die Planung und Inbetriebnahme einer Anlage zuständig ist. Betreiber von Anlagen verfügen häufig nicht über ausreichende Ressourcen für die Planung und Inbetriebsetzung von Neuanlagen oder für die Durchführung von Anlagenänderungen. Daher ist der Einsatz von Integratoren eine häufig geübte Praxis.
- Betreiber: Der Betreiber ist für den Betrieb und die Instandhaltung der Anlage verantwortlich. Möglicherweise delegiert der Betreiber Instandhaltungsaufgaben an Instandhaltungsdienstleister.

Die Teile 2 und 3 der VDI/VDE 2182 folgen dem beschriebenen Rollenkonzept. Im Teil 2 werden am Beispiel einer Produktionsanlage im Bereich der Fertigungsautomatisierung für die Rollen von Hersteller [VDI_2182_2_1], Integrator [VDI_2182_2_2] und Betreiber [VDI_2182_2_3] die Aufgaben gemäß des in Teil 1 beschriebenen Vorgehensmodells beschrieben. Das gleiche findet sich im Teil 3 für eine Anlage der Prozessautomatisierung in gleicher Weise [VDI_2182_3_1] [VDI_2182_3_2] [VDI_2182_3_3].

Mit der VDI/VDE 2182 Normreihe steht Herstellern, Integratoren und Betreibern eine Basis zur Verfügung. Das Dokument bietet eine auf die jeweiligen Zuständigkeiten fokussierte Sicht auf das beschriebene PDCA-Vorgehensmodell. Die jeweiligen Teile führen an Hand eines realen Beispiels durch den Prozess und zeigen durch die Bereitstellung von Checklisten auf, in welcher Form eine Dokumentation der Ergebnisse erfolgen kann

3.2.3. VDS 3473-Teil 2

Der Leitfaden, zur Interpretation und Umsetzung der VdS 3473 L 1 für Industrielle Automatisierungssysteme, richtet sich speziell an kleine und mittelständische Unternehmen und stellt einer Ergänzung zu der bereits bestehenden Richtlinie [VDS_3473] dar. Der Teil 2 richtet sich an KMU, welche Produktionsanlagen betreiben. In einer knappen und übersichtlichen Form werden die Kriterien beschrieben, welche für die Umsetzung einer IT-Sicherheitsstrategie im Produktionsbereich erforderlich sind.

3.2.4. Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik bietet eine Reihe von Leitlinien im Bereich der IT-Sicherheit für Produktionsanlagen. In regelmäßigen Abständen veröffentlicht das BSI die Top-10-Bedrohungen für Automatisierungssysteme

[BSI2016a]. Darüber hinaus bietet das BSI mit dem ICS-Kompendium [BSI2013] einen Einstieg in die IT-Sicherheit von Produktionsanlagen für Anlagenbetreiber. Das Dokument „Anforderungen an netzwerkfähige Industriekomponenten" [BSI2014c] richtet sich an die Hersteller von Automatisierungskomponenten und definiert Anforderungen an Komponenten von Automatisierungssystemen. Neben diesen grundlegenden Dokumenten veröffentlicht das BSI in regelmäßigen Abständen Fallbeispiele, in denen spezielle Aspekte aufgegriffen werden. So gibt es z. B. Fallbeispiele für Angriffe [BSI2014d], ein Beispiel für den Einsatz von Servicetechnikern [BSI2014b] und IP-Kameras [BSI2016b]. Mit dem Software-Werkzeug LARS-ICS [BSI2014a] bietet das BSI zudem ein Software-Werkzeug an, welches für den in Kapitel 3.2.2 beschriebenen PDCA-Zyklus unterstützt.

Das Thema Remote Service und Remote Diagnose ist von besonderer Bedeutung, da hier aus dem Automatisierungsbereich Kommunikationsverbindungen über das Internet zu Dritten betrieben werden. Das BSI widmet diesem Thema ein separates Dokument [BSI-CS_108].

3.2.5. Leitlinien von Herstellerorganisationen

Industrielle Kommunikationssysteme wie PROFINET oder EtherNet/IP stellen einen wichtigen Teil einer Automatisierungsinfrastruktur dar. Aus diesem Grund haben die verschiedenen Herstellerorganisationen das Thema IT-Sicherheit in Produktionsanlagen adressiert und entsprechende Leitlinien herausgebracht. So bietet die PROFIBUS-Nutzerorganisation eine Leitlinie für PROFINET [PNO2013]. Ein vergleichbares Dokument steht von der ODVA für EtherNet/IP [ODV2011] zur Verfügung. In der aktuellen Ausgabe der Norm für das in der Gebäudeautomatisierung eingesetzte Bus-Protokoll BACNET [ISO16484-5] wurde bereits ein Kapitel IT-Sicherheit aufgenommen. Des Weiteren liegt für OPC UA ein Security-Modell als Technical Report der IEC [IEC_62541-2] vor. Das Bundesamt für Sicherheit in der Informationstechnik hat dieses Konzept evaluiert und im Wesentlichen positiv bewertet [BSI2016d], [WIC2016].

3.2.6. Branchenspezifische Normen

Neben den Herstellervereinigungen befassen sich auch Anwendervereinigungen mit dem Thema IT-Sicherheit. Die Interessengemeinschaft Automatisierungstechnik in der Prozessindustrie (NAMUR) hat sowohl eine Empfehlung zur IT-Sicherheit [NA_115] in bestehenden Anlagen als auch einen Ausblick auf künftige Anforderungen [NE_153] in Bezug auf die IT-Sicherheit in Automatisierungssystemen der Prozessindustrie herausgegeben.

Dem maritimen Sektor stehen z. B. mit Standards des American Bureau of Shipping (ABS) [ABS2016] und des Baltic and International Maritime Council (BIMCO) [BIM2016] ebenfalls branchenspezifisches Standards zur Verfügung.

Für den Sektor Energieversorgung und Energieverteilung können die Standards des North American Electric Reliability Corporation referenziert werden. Hier ist eine Reihe von Cyber Security Standards verfügbar [NERC2016]. Es ist zu beachten, dass gerade der Bereich der Energieversorgung auch durch nationale gesetzliche Regelungen geprägt ist.

An dieser Stelle kann lediglich ein begrenzter Ausblick auf branchenspezifische Normen gegeben werden, die keinen Anspruch auf Vollständigkeit hat.

3.2.7. Zusammenfassung Normen und Standards

Allen zuvor beschriebenen Dokumenten liegt der „Plan-Do-Check-Act-Zyklus" (PDCA-Zyklus) zu Grunde. In einem strukturierten Vorgehen werden, wie in Kapitel 3.2.2 beschrieben, die Assets erfasst, die Bedrohungen identifiziert, die Risiken bewertet und die notwendigen Maßnahmen abgeleitet, implementiert und verifiziert. Ein weiteres gemeinsames Kriterium ist die Etablierung einer IT-Sicherheitsstrategie im Unternehmen, die eine ganzheitliche und übergreifende Betrachtung einfordert. Neben technischen Aspekten sind insbesondere auch organisatorische und personelle Aspekte zu berücksichtigen.

In Bezug auf die technische Implementierung gehen die bestehenden Standards von einer Defense in Depth Strategie aus. Durch eine Reihe sich ergänzender Maßnahmen werden die Assets gegen Bedrohungen von außen abgeschottet und so geschützt.

Mit der Einführung von Industrie 4.0 werden die bestehenden Konzepte erweitert und verbessert werden müssen. In [NIE2014_1] werden eine Reihe von zusätzlichen Herausforderungen definiert, welche künftig in Bezug auf die IT-Sicherheit im Produktionsbereich zu adressieren sind. Dies sind insbesondere:

- Schutz gegen Innentäter
- Zunehmende Kommunikation auch über Unternehmensgrenzen hinweg
- Zugangskontrolle zum Netzwerk
- Absicherung der Kommunikation mit kryptografischen Mitteln.

Kapitel 5 wird diesen Aspekt noch einmal aufgreifen und diskutieren.

3.3. Das IT-Sicherheitsgesetz

Mit dem IT-Sicherheitsgesetz [ITSichG2015] definiert der Gesetzgeber Vorgaben in Bezug auf die IT-Sicherheit kritischer Infrastrukturen (KRTIS). Die Definition der kritischen Infrastrukturen ist dabei durch eine gesonderte Rechtsverordnung [BSI-KritisV] geregelt. In der aktuellen Ausgabe dieser Verordnung fallen die folgenden Infrastrukturen unter das Gesetz: Stromversorgung, Gasversorgung, Kraftstoff und Heizölver-

sorgung, Fernwärmeversorgung, Abwasserbeseitigung, Trinkwasserversorgung. Die Verordnung definiert Schwellenwerte für die Versorgungseinrichtungen. So fallen z. B. Kläranlagen ab 500 000 Einwohnerwerten oder Kraftwerke ab 420 MW Nennleistung unter die Verordnung. Es ist davon auszugehen, dass die Verordnung künftig den adressierten Kreis der Infrastrukturen erweitern wird.

Im Rahmen des IT-Sicherheitsgesetzes wird beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Meldestelle für Vorfälle eingerichtet und eine Meldepflicht für kritische Vorfälle definiert.

Weiterhin legt das Gesetz fest:

> *„Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtverordnung nach §10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.*" [ITSichG2015]

Die Betreiber Kritischer Infrastrukturen werden zudem verpflichtet eine Kontaktstelle einzurichten und müssen die Erfüllung der Anforderungen nachweisen. Darüber hinaus sind im [ITSichG2015] eine Reihe weiterer Änderungen an anderen Gesetzen zusammengefasst, welche einen Bezug zum Thema kritische Infrastrukturen und IT-Sicherheit haben.

Die Gesetzeslage wird dazu führen, dass sich die Betreiber kritischer Infrastrukturen zunehmend an ihre Lieferanten wenden werden, um Informationen und auch ggf. technische Ertüchtigungen von Komponenten einzufordern.

4. Maßnahmen zur Umsetzung der IT-Sicherheit in der Produktion

In Kapitel 3 wurde eine Übersicht über die relevanten Normen und Standards gegeben, um hieraus ein entsprechendes Vorgehen abzuleiten. Das Problem für KMU ist jedoch, dass diese Normenwerke sehr umfangreich und teilweise noch unvollständig sind. Daher fällt es KMU schwer zu einer Beurteilung in Bezug auf das eigene Unternehmen zu kommen. Eine erste Einschätzung kann ein Quick-Check liefern (z. B. www.vds-quick-check.de), der eine erste Einstufung des Unternehmens in Bezug auf die IT-Sicherheit liefert. Es stehen je ein Check für den Office- und den Produktionsbereich zur Verfügung.

Um KMU einen einfachen Einstieg in die IT-Sicherheit im Produktionsbereich zu ermöglichen, wird im Folgenden ein Zehn-Punkte-Plan für die Etablierung der IT-Sicherheit im Produktionsbereich vorgeschlagen. Diese zehn Punkte sind:

1. Management Commitment
2. Organisation der Zuständigkeiten und Prozesse
3. Erstellung einer Richtlinie
4. Schulung Personal
5. Beschaffung und Bereitstellung von Wissen
6. Identifizierung, Bewertung und Schutz der Assets
7. Regelung des externen Zugriffs auf Produktionsanlagen
8. Datensicherung
9. Behandlung von Störungen und Ausfällen
10. Behandlung von IT-Sicherheitsvorfällen

Die folgenden Kapitel werden sich mit diesen zehn Punkte befassen und notwendige Maßnahmen für die Etablierung eines IT-Sicherheitsprozesses im Produktionsbereich beschreiben. In der Regel fokussiert sich die Literatur stark auf die Punkte 6 und 7. Es ist jedoch festzuhalten, dass die IT-Sicherheit als gesamtheitlicher Prozess unter Einbeziehung aller Punkte anzusehen ist.

4.1. Management Commitment

Die IT-Sicherheit muss als Top-Down Prozess im Unternehmen etabliert werden. Nur durch ein entsprechendes Commitment des Managements ist eine Durchsetzung im Unternehmen sinnvoll. Hierfür sollte das Management eine IT-Sicherheitsstrategie für das Unternehmen verfassen (lassen), welche den Office- und den Produktionsbereich

umfasst. Die Strategie sollte klare Ziele und entsprechende Verantwortlichkeiten definieren.

Es wird empfohlen für die Initiierung des Prozesses ein Projekt zu definieren und es mit den erforderlichen internen und ggf. auch externen Ressourcen auszustatten. Das hier beschriebene Vorgehen ist vergleichbar zur Einführung eines Qualitätsmanagementprozesses.

4.2. Organisation der Zuständigkeiten und Prozesse

Nach dem Projektstart sind durch das Management entsprechenden Verantwortlichkeiten zu definieren. Da die IT-Sicherheit als übergreifender Prozess zu sehen ist, sollte eine Gesamtverantwortung in Form eines IT-Sicherheitsbeauftragten definiert werden. Es ist sicherzustellen, dass die Person über das erforderliche Wissen im Office- und im Produktionsbereich verfügt. Ggf. kann der IT-Sicherheitsbeauftragte Aufgaben delegieren. Der IT-Sicherheitsbeauftragte sollten gemeinsam mit weiteren Mitarbeitern und einem Vertreter des Managements das Informationssicherheitsteam bilden. Dieses Team ist für die Umsetzung der IT-Sicherheitsstrategie und für die Behandlung von Störungen, Ausfällen und IT-Sicherheitsvorfällen verantwortlich.

Zur Sicherstellung einer kontinuierlichen Arbeit ist dem Thema /dem Projekt entsprechendes Personal zuzuordnen. Die Berichtswege sind zu definieren. Die Delegation von Aufgaben und die Einbindung des Top-Managements sollten ebenfalls geregelt sein. Es ist zu beachten, dass auch Lieferanten und Systemintegratoren in die Prozesse mit einzubeziehen sind.

4.3. Erstellung einer Richtlinie

Das Thema IT-Sicherheit ist vom Unternehmen in einer entsprechenden Richtlinie, die dem Personal grundlegende Verhaltensregeln aufgeben, zu beschreiben. Nur wenn das Personal weiß, was von ihm in Bezug auf die IT-Sicherheit erwartet wird, kann es sich entsprechend verhalten. Dazu gehört die Vorgabe des Verhaltens der Mitarbeiter in Bezug auf die (Nicht-)Nutzung von Privatgeräten.

Für die Automatisierungssysteme ist insbesondere die Installation von Software, das Einbringen von Softwareaktualisierungen, sowie das vorherigen Prüfen von Softwareaktualisierungen zu definieren und den Umgang mit Schutzeinrichtungen (Fail Safe Systeme) zu beschreiben.

Die Richtlinie sollte auch den Informationsfluss bei Abwesenheit und die Weitergabe von Zugangskennungen beschreiben. Außerdem sollte sie klarstellen, dass eine Missbrauchskontrolle erfolgt und dass bei Fehlverhalten mit Sanktionen zu rechnen ist. Wie in Kapitel 4.2 sind auch hier Festlegungen für Lieferanten und Integratoren zu treffen.

4.4. Schulung Personal

Das Personal ist für die IT-Sicherheit ein entscheidender Faktor. Durch ein adäquates Knowhow und eine Ausbildung des Personals kann ein entscheidender Beitrag zur IT-Sicherheit im Unternehmen erfolgen.

Bei Eintritt in das Unternehmen ist eine Vertraulichkeitserklärung durch den Mitarbeiter bzw. die Mitarbeiterin zu unterzeichnen. In der Einarbeitungsphase sind neue Mitarbeiter in die Richtlinie zur IT-Sicherheit und evtl. weitere Richtlinien einzuweisen. Das Wissen des Personals ist durch Schulungen und Unterweisungen auf einem aktuellen Stand zu halten.

Bei dem Ausscheiden von Mitarbeitern sind entsprechende Maßnahmen zu treffen. VPN-Zugänge dieser Mitarbeiter sind zu sperren, Passworte sind zu ändern. Das gilt auch für Schichtzugänge.

4.5. Beschaffung und Bereitstellung von Wissen

In einem Bericht in der Fachpresse wurde im Jahr 2013 auf Schwachstellen in Komponenten von Automatisierungssystemen hingewiesen, die über das Internet erreichbar waren [STA2013b]. Eine Nachprüfung zwei Jahre später ergab, dass ein großer Teil der Systeme nach wie vor ungeschützt war [STA2015]. Die vom Hersteller bereitgestellten Softwareaktualisierungen wurden nicht in die Systeme eingespielt. Dieser Fall verdeutlicht, dass es für die Betreiber von Automatisierungssystemen essenziell ist, sich über bekannte Schwachstellen ihrer Systeme zu informieren und diese zu beheben.

Aus diesem Grund ist im Unternehmen ein Prozess zu etablieren, der die Beschaffung entsprechender, aktueller Informationen für das Unternehmen gewährleistet. Mögliche Quellen für die Beschaffung von Informationen über Schwachstellen können sein:

- Informationen der Hersteller der Automatisierungssysteme. Zum Beispiel:
    - z. B. ABB [ABB2016]
    - z. B. Siemens [SIE2016]

    - z. B. Wago: [WAG2017]
- Informationen von ICS-CERT (Homeland Security der U.S.A) bezüglich bekannter Schwachstellen von Automatisierungssystemen [DHS2016a]
- Datenbanken mit bekannten Schwachstellen. Zum Beispiel:
    - CVE Common Vulnerabilities and Exposures [MIT2016]
    - Open Indicators of Compromise (Open IOC) [MAN2016]

Die Aktualität des Wissens ist sicherzustellen. In einigen Fällen besteht die Möglichkeit Alerts (Meldungen über vom Hersteller erkannte Schwachstellen) für bestimmte Systeme über einen Email-Verteiler zu abonnieren. Im Unternehmen sind Personen zu benennen, welche diese Meldungen auswerten und Maßnahmen für das Unternehmen daraus ableiten.

Neben dem spezifischen Wissen in Bezug auf bekannte Schwachstellen ist das allgemeine Wissen der Mitarbeiterinnen und Mitarbeiter durch Sensibilisierung, Aus- und Weiterbildung zu etablieren und auf einem aktuellen Stand zu halten.

4.6. Identifizierung, Bewertung und Schutz der Assets

Dieser Abschnitt beschreibt wie die Assets einer Produktionsanlage systematisch erfasst, bewertet und bei Bedarf geschützt werden. Hierbei wird gemäß der Normreihe VDI 2182 vorgegangen. Die Normreihe IEC 62443 gibt ein vergleichbares Vorgehen wieder. Für die Analyse des Automatisierungssystems wird in den in Abbildung 5 dargestellten Schritten vorgegangen. Kapitel 3.2.2 beschreibt den „Plan-Do-Check-Act-Zyklus" (PDCA) und die notwendigen Schritte.

Das Ergebnis dieser Analyse ist:

- Liste aller Assets
- Aufstellung der Bedrohungen, welche auf die Assets wirken in Form einer Bedrohungsmatrix.
- Liste aller relevanten Schutzziele in Form einer Bedrohungsmatrix mit relevanten Schutzzielen.
- Liste der bewerteten Risiken, welche auf die Assets wirken.
    - Die Normreihe VDI 2182 macht Vorschläge für den Aufbau derartiger Listen.
- Liste von möglichen Schutzmaßnahmen und Bewertung von deren Wirksamkeit und deren Kosten.
- Liste der ausgewählten und zu realisierenden Schutzmaßnahmen.
- Bericht über die Umsetzung der Schutzmaßnahmen
- Ergebnisse des Prozessaudits zur Beurteilung der Wirksamkeit der gewählten Maßnahmen.

Typische Schutzmaßnahmen, die das Ergebnis des beschriebenen Prozesses sind, resultieren in der Regel in einem so genannten Defense in Depth Konzept [DHS2016b]. Die folgenden Abbildungen zeigen exemplarisch ausgewählte Bestandteile eines Defense in Depth Konzeptes.

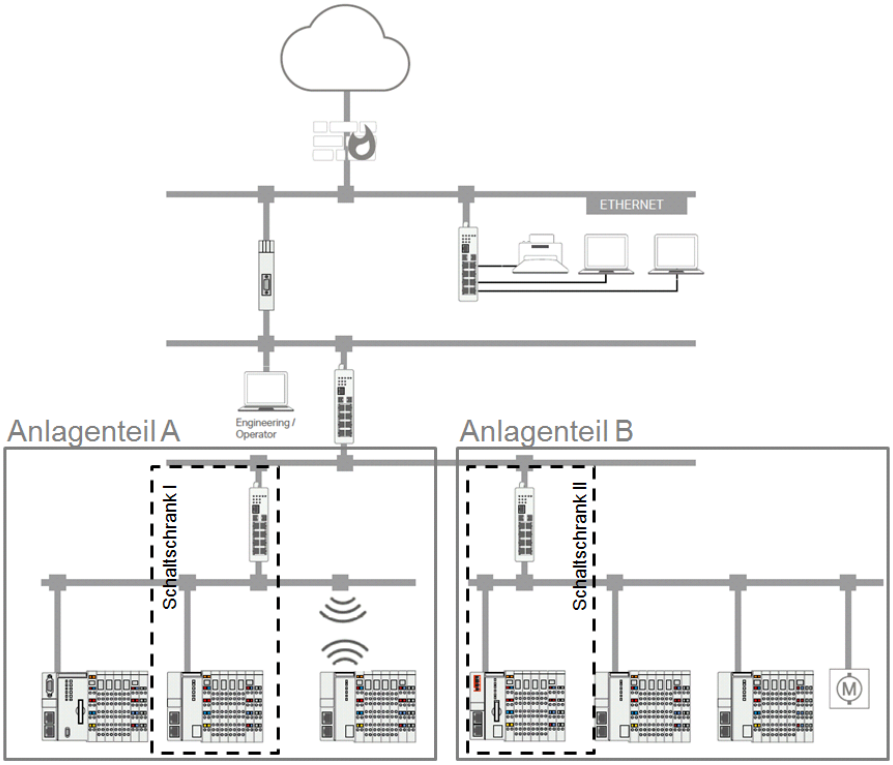

Abbildung 6: Beispielanlage mit Office und Produktionsbereich

Abbildung 6 zeigt eine aus zwei Teilen bestehende Produktionsanlage. Oberhalb der Produktionsanlage ist der Bereich der Leitwarte angesiedelt. Darüber ist der Office-Bereich dargestellt. Es wird davon ausgegangen, dass das Unternehmen durch eine Firewall vom Internet getrennt ist. Eine Verbindung zum Internet wird z. B. für den Bezug von Software-Updates oder für die Speicherung von Daten in der Cloud benötigt.

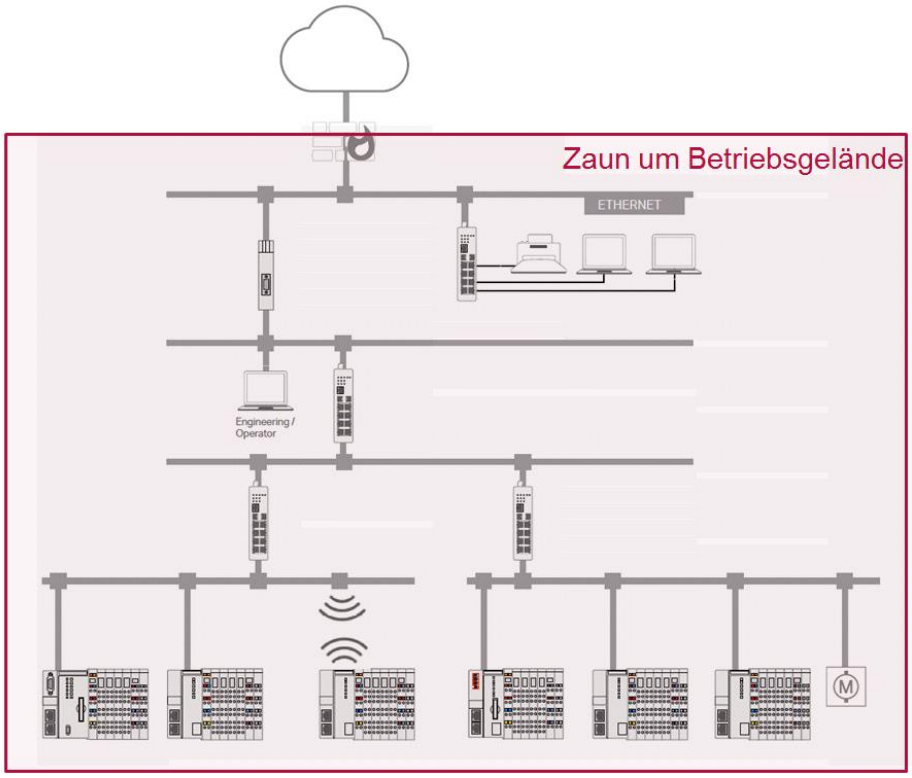

Abbildung 7: Perimeterschutz

Als erste Maßnahme kann, wie in Abbildung 7 dargestellt, die gesamte Liegenschaft gegen Eindringen von außen, z. B. durch einen Zaun geschützt werden. Diese Maßnahme verhindert den Zugang unautorisierter Personen zum Werksgelände und stellt die erste Barriere für Angreifer dar. Es ist allerdings ein Vorfall bekannt, bei dem ein Cyber-Angreifer einen doppelten Zaun überwinden und durch einen Cyber-Angriff ein Kraftwerk stilllegen konnte [PAN2008]. Das bedeutet, dass der Zaun nur eine von mehreren ineinandergreifenden Maßnahmen sein kann.

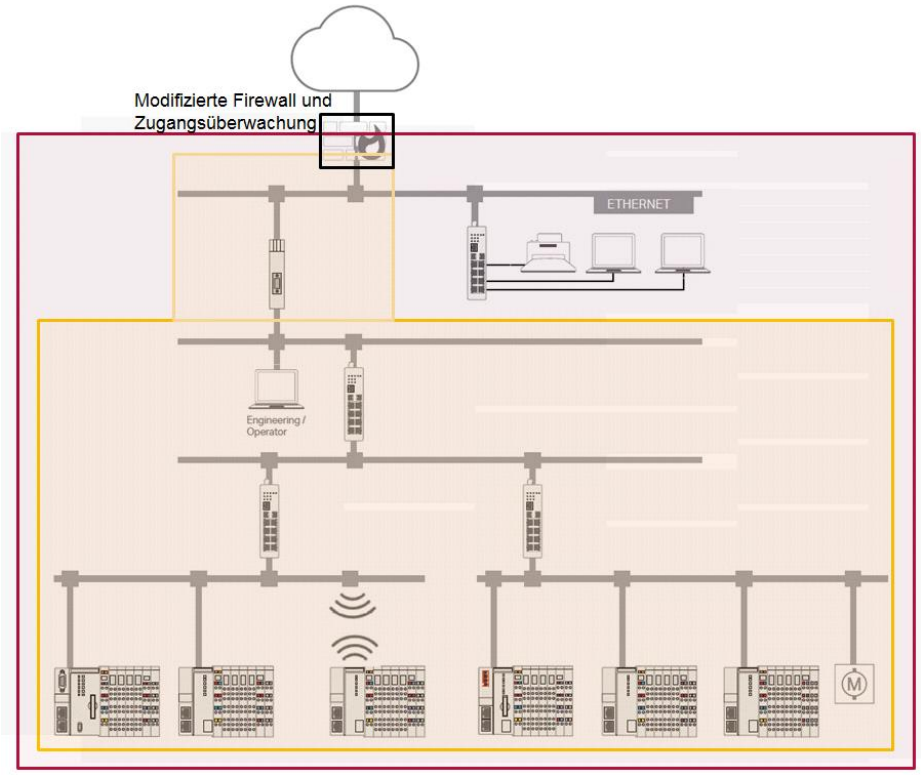

Abbildung 8: Modifizierte Firewall und Zugangsüberwachung Gebäude

Abbildung 8 zeigt als nächste Schutzmaßnahme eine geänderte Konfiguration der Firewall. Diese wird nun so konfiguriert, dass kein Zugang zum Automatisierungssystem von außerhalb der Firma zulässig ist. Gleichzeitig werden für den Betrieb der Anlage notwendige Verbindungen in den Office-Bereich zugelassen. Als weitere Maßnahme wird eine Zugangsüberwachung für das Gebäude installiert, in dem sich die Produktionsanlage befindet. Durch diese Maßnahmen wird der Produktionsbereich vom Office-Bereich und vom Internet datenmäßig getrennt. Zusätzlich zum Zaun um das Werksgelände ist ein zweiter, enger gefasster Zugangsschutz realisier worden.

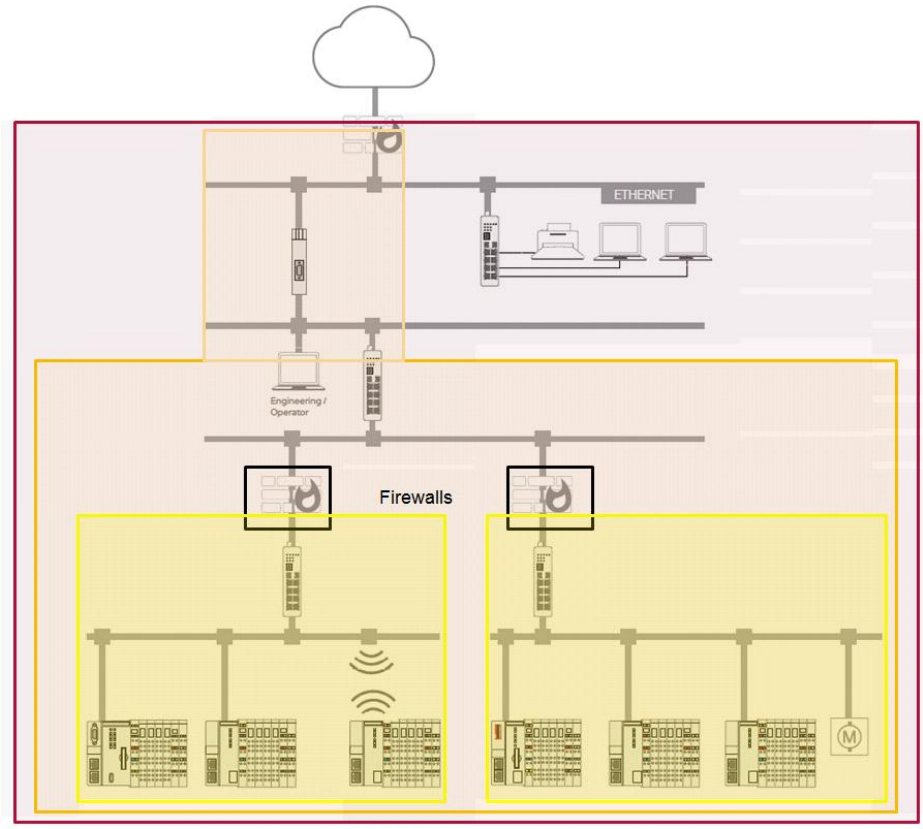

Abbildung 9: Abschottung des Produktionsbereichs

Abbildung 9 zeigt eine weitere Untergliederung der Produktionsanlage. Produktionsanlage wird in zwei Teilbereiche unterteilt (gelber Hintergrund). Jeder dieser Bereiche wird wiederum über eine Firewall vom Wartenbereich (ockerfarbener Hintergrund) getrennt. Zusätzlich könnten die Komponenten in den Teilbereichen z. B. durch Einbau in einen verschlossenen Schaltschrank weiter geschützt werden.

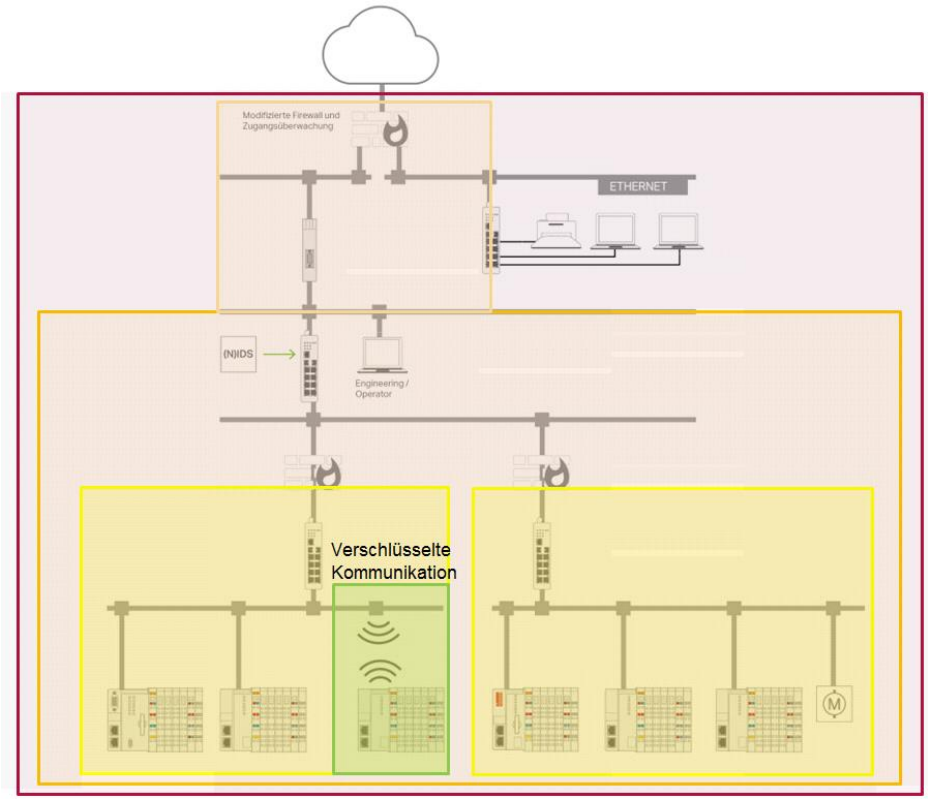

Abbildung 10: Verschlüsselung der Kommunikation

Abbildung 10 zeigt die Schutzmaßnahme für einen drahtlosen Zugangspunkt durch Verschlüsselung. Auch wenn marktgängige WLAN-Access-Points standardmäßig eine Verschlüsselung bieten, ist auf die Wahl eines ausreichend sicheren Verfahrens und auf ausreichend starke Passworte zu achten.

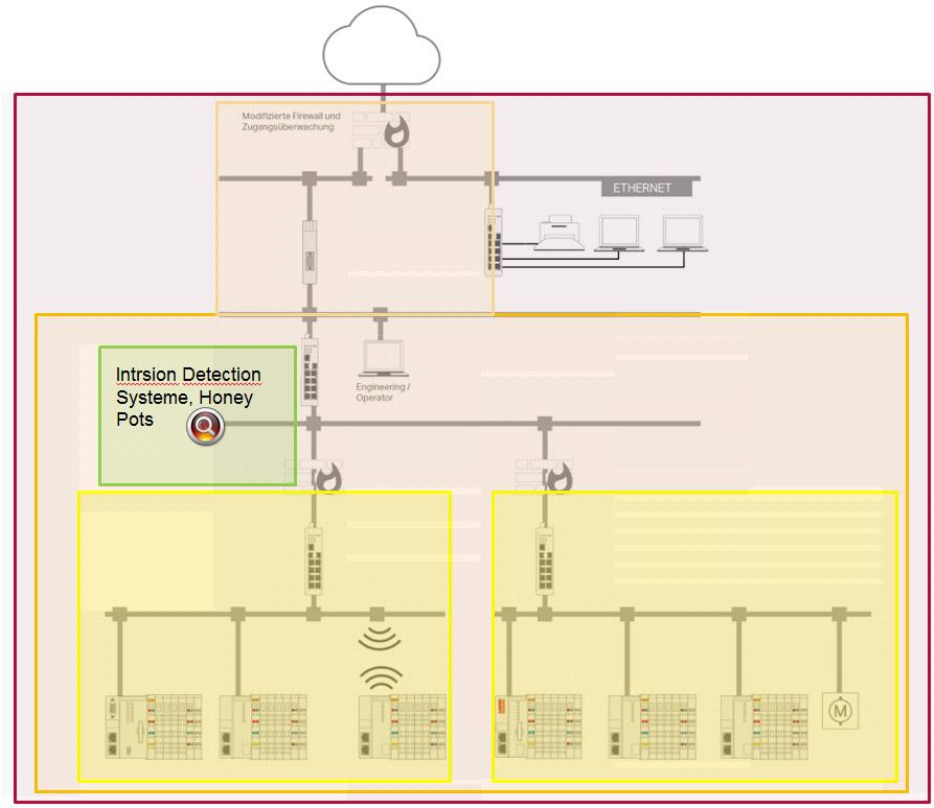

Abbildung 11: Netzwerküberwachung

Abbildung 11 zeigt als letzte Maßnahme die Überwachung z. B. über einen Honey Pot oder über ein Netzwerküberwachungssystem. Der Honey-Pot ist ein Überwachungssystem welches sich als einfaches Opfer ausgibt und mögliche Angreifer anlockt und Angriffe dokumentiert und meldet. Ein Netzwerküberwachungssystem (Network Intrusion Detection System-NIDS bzw. Intrusion Detection System-IDS) überwacht den Netzwerkverkehr auf Anomalien.

Die hier vorgestellten Maßnahmen stellen einige exemplarische Beispiele dar. Es existieren weitere Maßnahmen auf die an dieser Stelle aus Platzgründen nicht weiter eigegangen wird. Beispiele hierfür sind z. B:

- Virenschutz
- Applikations-Whitelisting
- Zugangsbeschränkung für transportable Medien
- Einrichtung von demilitarisierten Zonen (DMZ) für das Einbringen von Softwareupdates.
- Authentifizierung von Netzwerketeilnehmern
- Begrenzung des Zugangs zum Netz durch Abschalten unbenutzter Netzwerk-Ports.

Obwohl dieser Teil des Zehn-Punkte-Programms der aufwendigste ist, sollten die anderen Punkte nicht gegenüber diesem Teil vernachlässigt werden.

4.7. Regelung des externen Zugriffs auf Produktionsanlagen

Der externe Zugriff auf Produktionsanlagen für Remote-Diagnose- und Remote-Wartungs-Zwecke ist aus Sicht der IT-Sicherheit ein besonders kritischer Vorgang. Aus diesem Grund wird dieses Thema in einem separaten Abschnitt beschrieben.

Bekannte Vorfälle dieser Art gehen auf die Nutzung von Remote-Zugängen zurück [BYR2009] [SAN2016]. Aus diesem Grund gelten für diese Zugänge besondere Sicherheitsmaßnahmen. Eine gute Orientierung kann [BSI-CS_108] geben. Hier beschreibt das BSI die grundlegenden Vorgehensweisen für die Errichtung von Remote-Zugängen. Die wesentlichen Vorgaben des BSI sind:

- Einheitliche Lösung errichten. Dies standardisiert die verwendete Hardware und die genutzten Prozesse und reduziert so den Verwaltungsaufwand.
- Anordnung der Fernwartungskomponenten in einer vorgelagerten Zone (DMZ).
- Kein pauschaler Zugriff auf ein ganzes (Sub-)Netz sondern nur auf dedizierte Endpunkte.
- Aufbau der Verbindung aus dem Unternehmen heraus nach außen.
- Einsatz dedizierter Systeme, die nur für diesen Zweck verwendet werden.
- Es werden ausschließlich etablierte Protokolle wie IPsec, SSH oder SSL/TLS in aktuellen Versionen eingesetzt, um einen Tunnel zwischen zwei Endpunkten bzw. Netzen herzustellen.
- Die Verbindung zwischen Unternehmen und Diagnosestelle ist zu verschlüsseln. Es werden hinreichend starke kryptographische Verfahren zur Verschlüsselung verwendet.
- Es sollte nur ein Benutzer pro Account vorgesehen werden. Gruppen-Accounts sind unbedingt zu vermeiden.
- Verwendung von Multi-Faktor-Authentifizierungsverfahren.
- Bei Einsatz von Passworten sind entsprechende Vorgaben zu erstellen und zu beachten.
- Mechanismen zur Detektion von Angriffen auf Passwort-basierte Authentisierungsverfahren sind zu verwenden.
- Erstellen einer Risikoanalyse.
- Beachten des Minimalitätsprinzips (So wenige Verbindungen, wie möglich).
- Etablierung von Prozessen zur Freigabe und Sperrung von Zugängen.
- Vorgaben für das Personal, welches die Fernwartung durchführt. Z. B. Verbot die Fernwartung über Mobiltelefone durchzuführen.
- Begrenzung des Zugangs auf ein definiertes Zeitfenster. Automatische Trennung der Verbindung nach Ablauf einer bestimmten Zeitspanne.
- Einschalten und Auswerten von Protokollfunktionen.

Das referenzierte Dokument enthält noch weitere Informationen. In diesem Dokument werden lediglich die wesentlichen Punkte wiedergegeben.

4.8. Datensicherung

In [ZET2016] und [SAN2016] wird er Angriff auf das Ukrainische Energieversorgungsnetz im Jahr 2015 beschrieben. Unter anderem wurden bei diesem Angriff die Festplatten von Steuersystemen mit Hilfe der Software „KillDisk" unbrauchbar gemacht. Das Auslösen eines totalen Datenverlustes ist also eine schon heute bekannte Angriffsmethode. Aus diesem Grund kommt der Datensicherung im Produktionsbereich eine besondere Bedeutung bei.

Es ist ein Konzept für die Beherrschung eines katastrophalen Datenverlustes (Löschung aller Datenbestände einschließlich Betriebssystem) zu entwickeln. Bestandteil eines Datensicherungskonzeptes ist die regelmäßige und vollständige Sicherung aller Datenbestände des Automatisierungssystems. Die Wiederherstellungsroutinen sind zu dokumentieren und zu testen.

In Anbetracht der sich weiter ausbreitenden Verschlüsselungstrojaner wie z. B. Locky [MC 2016] sollten die Backupsysteme nur für die Dauer des Backups mit dem Rechnernetzwerk verbunden sein. Darüber hinaus sollten die Daten des Backupsystems nicht vom Rechnernetzwerk aus veränderbar oder löschbar sein.

4.9. Behandlung von Störungen und Ausfällen

Eine schnelle und effiziente Behandlung von Störungen und Ausfällen ist erforderlich, um nach einem solchen Vorfall den Betrieb schnell wieder aufnehmen zu können. Hierfür ist es maßgebend, dass der Begriff eindeutig definiert ist. Die Meldeart und die Meldewege sind festzulegen und zu dokumentieren. Es ist festzulegen, welche Art von Vorfällen in diese Kategorie fällt. Weiterhin ist ein Plan für eine Kommunikation nach außen zu erstellen. Die Reaktionen auf Störungen und Ausfälle sind zu definieren und Vorgehensmodelle (Wiederanlaufpläne) zur Beherrschung derartiger Störfälle sind erforderlich.

Bei Auftreten hat zunächst die Wiederherstellung des ordnungsgemäßen Betriebs die höchste Priorität. Danach erfolgen eine Ursachenuntersuchung, eine Dokumentation des Schadens sowie die Nachbereitung zur Abwendung künftiger Vorfälle.

4.10. Behandlung von IT-Sicherheitsvorfällen

Die in Kapitel 4.9 beschriebenen Störungen können zunächst allgemeiner Art sein. Die IT-Sicherheitsvorfälle bilden eine Unterkategorie dieser Vorfälle, die einer besonderen Behandlung bedürfen. Grundsätzlich gilt für IT-Sicherheitsvorfälle zunächst das in Kapitel 4.9 beschriebene Vorgehen. Zusätzlich sind zum Erkennen und Abwenden von IT-Sicherheitsvorfällen präventive Maßnahmen sinnvoll. Eine Befragung des SANS-Institute [SAN2015] ergab, dass 15% der befragten Unternehmen angaben, mehr als einen Monat für das Erkennen eines Befalls benötigt zu haben.

Aus diesem Grund sind weiterreichende Maßnahmen wie z. B. Eine Netzwerkzugangsüberwachung, eine (ggf. automatisierte) Auswertung von Logfiles, Honey Pots oder Netzwerküberwachungssysteme (Intrusion Detection Systems) sinnvoll. In jedem Fall sollte ein unternehmensinternes Meldesystem zur Erfassung und Behandlung von IT-Sicherheitsvorfällen aufgebaut werden.

5. Ausblick

Der in Kapitel 4 vorgestellte 10-Punkte-Maßnahmenplan bietet einen ersten Ansatz zur Umsetzung der IT-Sicherheit im Produktionsbereich. Obwohl er geeignet ist einen ausreichenden Schutz für eine Produktionsanlage zu realisieren, bestehen dennoch einige Defizite, die im Kontext von Industrie 4.0 stärker hervortreten werden.

Die dem Stand der Technik entsprechenden Maßnahmen weisen die folgenden Defizite auf:

- Die Konzepte fokussieren stark auf die Abwehr von „Außen". In [HAR2015] wird dargestellt, dass die Beschäftigen mit 25% der Vorfälle die größte Tätergruppe darstellen. Künftige Konzepte müssen sich also stärker als bisher auf einen Schutz gegen Innentäter konzentrieren.
- Jeder Angreifer, der Zugang zu einem ungesicherten Netzwerk-Switch hat, kann ein Gerät in das Netzwerk einbringen und an der Kommunikation teilnehmen. In [LIN2014] wird eindrucksvoll beschrieben, wie ein Angreifer durch einen ungesicherten Netzwerkzugang die Kontrolle über ein Automatisierungssystem erlangen konnte.
- Die zunehmende horizontale und vertikale Integration im Kontext von Industrie 4.0 wird dazu führen, dass die klassischen Schutzmechanismen nur noch eingeschränkt wirksam sein werden. Die Anzahl der Netzwerkknoten wird zunehmen, der Aufwand für die Sicherstellung der IT-Sicherheit wird steigen.

Die NAMUR hat in [NE_153] Anforderungen an künftige Automatisierungssysteme beschrieben. Der wesentliche Grundgedanke ist der „Security by Design" Ansatz. Statt einer Abschottung der Geräte werden künftig Sicherheitsfunktionen in die Geräte integriert, welche eine sichere Kommunikation auch unter Echtzeitbedingungen erlauben werden. Wesentliche Anforderungen für ein solches Konzept finden sich in [NIE2014_1] oder [NIE2014_2].

Für die Umsetzung der IT-Sicherheit heute sollten jedoch die gängigen Maßnahmen realisiert werden und insbesondere die „low hanging fruits", die mit beschränktem Aufwand erreichbaren Ziele, geerntet werden. Hier kann mit geringem Aufwand ein großer Gewinn an Sicherheit erzielt werden.

6. Abbildungsverzeichnis

7. Tabellenverzeichnis

8. Literaturverzeichnis

[ABB2016] ABB Asea Brown Boveri Ltd: Cyber security alerts and notifications. http://new.abb.com/about/technology/cyber-security/alerts-and-notifications, 29.11.2016.

[ABS2016] American Bureau of Shipping: Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations - Volume 1: Cybersecurity. http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/221_Guidance_Notes_Cyber_Safety_Principles_Maritime_Operations/Cyber_Security_v1_GN_e.pdf, 08.03.2016.

[BIM2016] BIMCO: The Guidelines on Cyber Security onboard Ships. https://www.bimco.org/News/2016/01/~/media/AEEEE215CBE3421F8F7493A6A1B0E521.ashx.

[BRO2011] Broad, William J.; Markoff, John, Sander, David E.: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&sq=stux.

[BSI2013] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile, 05.06.2014.

[BSI2014a] LARS ICS. Light and Right Security ICS - Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security -Benutzerhandbuch, Bonn, 2014a.

[BSI2014b] Bundesamt für Sicherheit in der Informationstechnik: Empfehlung IT in der Produktion. Fallbeispiel Schwimmbad. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/materialien/fallbeispiele/BSI-CS_095a.pdf?__blob=publicationFile, 29.07.2015.

[BSI2014c] Bundesamt für Sicherheit in der Informationstechnik: Anforderungen an netzwerkfähige Industriekomponenten. https://www.bsi.bund.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_067.pdf;jsessionid=320A5E59D3035F5560291B16C049C738.2_cid286?__blob=publicationFile, 15.06.2014.

[BSI2014d] Bundesamt für Sicherheit in der Informationstechnik: Fallbeispiel Servicetechniker. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/materialien/fallbeispiele/BSI-CS_095c.pdf?__blob=publicationFile, 29.07.2015.

[BSI2014e] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/bsi-lagebericht-it-sicherheit.pdf%3F__blob%3DpublicationFile, 12.01.2015.

[BSI2016a] Bundesamt für Sicherheit in der Informationstechnik: Top 10 Bedrohungen und Gegenmaßnahmen 2016. Industrial Control System Security. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4.

[BSI2016b] Bundesamt für Sicherheit in der Informationstechnik: Sicherheit von IP-basierten Überwachungskameras. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_128.pdf?__blob=publicationFile&v=5.

[BSI2016c] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzkataloge. 15. Ergänzungslieferung. https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf.

[BSI2016d] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheitsanalyse OPC UA. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2.

[BSI-CS_108] Bundesamt für Sicherheit in der Informationstechnik: Fernwartung im industriellen Umfeld. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf?__blob=publicationFile&v=3, 15.01.2015.

[BSI-KritisV]: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung). BSI-KritisV, 2016.

[BYR2009] Byres security lnc.: Daimler Chrysler Cyber Security lncident case Profile. Virus shuts down 13 plants; loss estimated at $14 million. https://www.tofinosecurity.com/sites/default/files/CP-104-Case_Profile-Daimler_Chrysler-rev1.pdf.

[CERT2014] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Alert (ICS-ALERT-14-176-02A). ICS Focused Malware (Update A). https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A, 13.11.2014.

[CERT2016] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Cyber-Attack Against Ukrainian Critical Infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[DEU2015] Deutsche Telekom /T-Systems: Cyber Security Report 2015. Ergebnisse einer repräsentativen Befragung von Abgeordneten sowie Top-Führungskräften in mittleren und großen Unternehmen. https://www.telekom.com/static/-/293656/2/Cyber-Security-Report-2015-si, 22.11.2015.

[DHS2016a] Department of Homeland Security: ICS-CERT Alerts. https://ics-cert.us-cert.gov/alerts, 29.11.2016.

[DHS2016b] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[DIR2015] DiRenzo, Joseph; Goward, Dana A.; Fred S. Roberts: The Little-known Challenge of Maritime Cyber Security: 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 2015.

[EIK2013] Eikenberg, Ronald: Vaillant-Heizungen mit Sicherheits-Leck. http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html, 12.02.2016.

[FAL2011] Falliere, Nicolas; Murchu, Liam O.; Chien, Eric: W32.Stuxnet Dossier. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 21.08.2014.

[GLA2015] Glawe, M. Fay, A.; Tebbe, C.; Niemann, K.-H.; Schewe, F.: Wissensbasierte Methoden zur Erstellung von IT-Sicherheitsanalysen automatisierter Anlagen. In (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik Hrsg.): Automation 2015 - Benefits of Change – the Future of Automation. VDI-Verlag GmbH, Düsseldorf, 2015; S. Ohne Seitenzählung.

[HAR2015] Harp, Derek; Gregory-Brown, Bengt: The State of Security in Control Systems Today. http://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, 29.07.2015.

[ICS2016] ICS-CERT: Downloading and Installing CSET. https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET, 30.11.2016.

[IEC_62443_1_1] IEC- International Electrotechnical Commission IEC/TS 62443-1-1: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009.

[IEC_62443_1_2] IEC- International Electrotechnical Commission ISA-TR62443-1-2: Security for industrial automation and control systems - Master Glossary.

[IEC_62443_1_3] IEC- International Electrotechnical Commission IEC/TS 62443-1-3: Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics, 2014.

[IEC_62443_1_4] IEC- International Electrotechnical Commission ISA-62443-1-4: Security for industrial automation and control systems Life Cycle and Use Cases, 2013.

[IEC_62443_2_1] IEC- International Electrotechnical Commission IEC 62443-2-1-2010: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, 2010.

[IEC_62443_2_2] IEC- International Electrotechnical Commission ISA 62443-2-2: Security for industrial automation and control systems - Implementation Guidance for an IACS Security Management Systems, 2013.

[IEC_62443_2_3] IEC- International Electrotechnical Commission IEC/TR 62443-2-3: Industrial communication networks – Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment., 2014.

[IEC_62443_2_4] IEC- International Electrotechnical Commission IEC 62443-2-4: Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for IACS solution suppliers., 2014.

[IEC_62443_3_1] IEC- International Electrotechnical Commission ISA 62443-3-1: Technical Report Security Technologies for Industrial Automation and Control Systems, Rev. 2, 2007.

[IEC_62443_3_2] IEC- International Electrotechnical Commission IEC 62443-3-2: Industrial communication networks - Network and system security – Part 3-2: Security assurance levels for zones and conduits, 2013.

[IEC_62443_3_3] IEC- International Electrotechnical Commission ISA-62443-3-3 (99.03.03): Security for industrial automation and control systems Part 3-3: System security requirements and security levels, 2013.

[IEC_62443_4_1] IEC- International Electrotechnical Commission IEC/NP 62443-4-1: Industrial communication networks – Network and system security – Part 4-1: Product development requirements, 2013.

[IEC_62443_4_2] IEC- International Electrotechnical Commission IEC/NP 62443-4-2: Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components.

[IEC_62541-2] IEC- International Electrotechnical Commission IEC TR 62541-2:2016: OPC unified architecture - Part 2: Security Model, 2016.

[ISA2016] ISA - The International Society of Automation: ISA99 Committee - Work Product List. http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[ISO16484-5] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V DIN EN ISO 16484-5: Systeme der Gebäudeautomation – Teil 5: Datenkommunikationsprotokoll (ISO 16484-5:2014); Englische Fassung EN ISO 16484-5:2014. Beuth Verlag GmbH, Berlin, 2014.

[ITSichG2015]: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015.

[JEN2015] Jensen, Lars: Challenges in Maritime Cyber-Resilience. In Technology Innovation Management Review 04, 2015; S. 35–39.

[KER2013] Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner; Wolfenstetter, Klaus-Dieter: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung. Springer, Wiesbaden, 2013.

[KER2016] Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen; Schröder, Klaus-Werner: IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Springer Vieweg, Wiesbaden, 2016.

[KOB2016] Kobes, Pierre: Leitfaden Industrial Security. IEC 62443 einfach erklärt. VDE Verlag, Berlin, Offenbach, 2016.

[LAN2013] Langner, Ralph: To kill a centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, 13.11.2014.

[LIN2014] Lindner, Felix: Licht aus! Sicherheit kritischer Infrastrukturen im Test. In c't Magazin für Computertechnik 9, 2014; S. 150–155.

[MAN2016] Mandiant: Open IOC. http://openioc.org/.

[MC 2016] Mc Affee Labs: Threat Report September 2016. http://www.mcafee.com/de/resources/reports/rp-quarterly-threats-sep-2016.pdf.

[MIT2016] Mitre Corporation: Common Vulnerabilities and Exposures. https://cve.mitre.org/, 29.11.206.

[NA_115] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V: NA115: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie, 17.11.2016.

[NE_153] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V NE 153: Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme, Leverkusen, 2015.

[NERC2016] North American Electric Reliability Corporation (NERC): Critical Infrastructure Protecion (CIP) Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, 19.03.2016.

[NIE2014_1] Niemann, Karl Heinz: IT Security Konzepte. Anforderungen im Kontext von Industrie 4.0. In (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik Hrsg.): Automation 2015. Smart X - Powered by Automation. VDI-Verlag GmbH, Düsseldorf, 2014; S. 489–506.

[NIE2014_2] Niemann, Karl Heinz: IT-Security-Konzepte für die Prozessindustrie. Anforderungen im Kontext von Industrie 4.0. In atp-edition 7-8/2014, 2014, Jahrgang 56; S. 62–69.

[ODV2011] ODVA Inc.: Securing EtherNet/IP Networks. http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00269R0_ODVA_Securing_EtherNetIP_Networks.pdf, 28.04.2014.

[PAK2005] Pakalski, Ingo: Computerwurm befällt CNN, DaimlerChrysler und Walt Disney. http://www.golem.de/0508/39902.html.

[PAN2008] Pany, Thomas: Saboteur schaltet Turbine des britischen Kohlekraftwerks Kingsnorth aus. https://www.heise.de/newsticker/meldung/Saboteur-schaltet-Turbine-des-britischen-Kohlekraftwerks-Kingsnorth-aus-188799.html?view=print.

[PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Guideline7.002. http://www.profibus.com/download/specifications-standards/.

[SAN2015] SANS Institute: The State of Security in Control Systems Today. http://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, 19.07.2016.

[SAN2016] SANS Institute: Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[SIE2016] Siemens Aktiengesellschaft: ProductCERT Security Advisories. http://www.siemens.com/cert/de/cert-security-advisories.htm, 29.11.2016.

[STA2013a] Stahl, Louis-F.; Eikenberg, Ronald: Fünf nach zwölf. Die „Gefahr im Kraftwerk" ist noch nicht gebannt. In c't Magazin für Computertechnik 15, 2013a; S. 16–17.

[STA2013b] Stahl, Louis-F.: Gefahr im Kraftwerk. Industrieanlagen schutzlos im Internet. In c't Magazin für Computertechnik 11, 2013b; S. 78–82.

[STA2015] Stahl, Louis-F.; Benz, Benjamin; Eikenberg, Ronald: Risiko verdrängt und vergessen. Industriesteuerungen nach über zwei Jahren noch verwundbar. In c't Magazin für Computertechnik 21, 2015; S. 86–87.

[VDI_2182_3_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 3.1: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller Prozessleitsystem einer LDPE-Anlage. Beuth Verlag, Berlin, 2013.

[VDI_2182_3_2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 3.2: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren LDPE-Reaktor. Beuth Verlag, Berlin, 2013.

[VDI_2182_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 1: Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Beuth Verlag, Berlin, 2011.

[VDI_2182_2_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 2.1: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller Speicherprogrammierbare Steuerung (SPS). Beuth Verlag, Berlin, 2013.

[VDI_2182_2_2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 2.2: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer Umformpresse. Beuth Verlag, Berlin, 2013.

[VDI_2182_2_3] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer Umformpresse. Beuth Verlag, Berlin, 2011.

[VDI_2182_3_3] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 3.3: Informationssicherheit in der industriellen Automatisierung Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage. Beuth Verlag, Berlin, 2013.

[VDS_3473] VdS Schadenverhütung GmbH: Informationssicherheit in kleinen und mittleren Unternehmen (KMU). Anforderungen. http://www.vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf.

[WAG2017] WAGO Kontakttechnik GmbH & Co. KG: Wago Security-Hinweise Automatisierungskomponenten. http://www.wago.de/produkte/produktkatalog/automatisierungskomponenten/security-hinweise/index.jsp, 02.02.2017.

[WIC2016] Wichmann, Andre: Sicherheitsanalyse von OPC UA für Industrie 4.0. In atp edition 07-08, 2016, Jahrgang 58; S. 40–45.

[ZET2016] Zetter, Kim: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 05.03.2016.